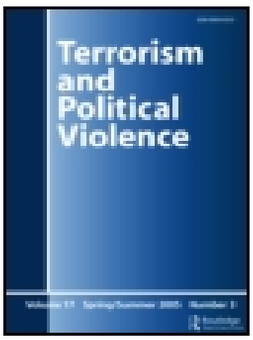

Terrorism and Political Violence

ISSN: 0954-6553 (Print) 1556-1836 (Online) Journal homepage: https://www.tandfonline.com/loi/ftpv20

Examining Ideologically Motivated Cyberattacks Performed by Far-Left Groups

Thomas J. Holt, Mattisen Stonhouse, Joshua Freilich & Steven M. Chermak

To cite this article: Thomas J. Holt, Mattisen Stonhouse, Joshua Freilich & Steven M. Chermak (2019): Examining Ideologically Motivated Cyberattacks Performed by Far-Left Groups, Terrorism and Political Violence, DOI: 10.1080/09546553.2018.1551213

To link to this article: https://doi.org/10.1080/09546553.2018.1551213

Published online: 24 Jan 2019.

TERRORISM AND POLITICAL VIOLENCE
https://doi.org/10.1080/09546553.2018.1551213

Routledge
Taylor & Francis Group

Examining Ideologically Motivated Cyberattacks Performed by Far-Left Groups

Thomas J. Holt[a], Mattisen Stonhouse[b], Joshua Freilich[c] and Steven M. Chermak[d]

[a]School of Criminal Justice, Michigan State University, East Lansing, Michigan, USA; [b]Northeastern University, Boston, Massachusetts, USA; [c]Criminal Justice, John Jay College, New York, NY, USA; [d]Criminal Justice, Michigan State University, East Lansing, Michigan, USA

ABSTRACT

Over the last two decades, there has been a massive increase in research examining terror and extremist-related violence. Few have considered the extent to which these same groups may engage in attacks against digital infrastructure and the Internet, whether through hacking or other methods. The absence of empirical evidence calls to question the nature and dynamics of cyberattacks performed by extremists and ideologically motivated actors. This study attempted to address this gap in the literature through a qualitative investigation of 26 attacks performed by far-left groups against targets in the UK, US, and Canada from 2000 to 2015. This data was compared to physical attacks documented in the Extremist Crime Database during the same period. The findings demonstrated that there was an increase in cyberattacks during a period of decreased physical violence by far-left groups. Additionally, there was some parity in the targets of far-left groups on- and off-line, with similar motivations to cause harm to or embarrass businesses, government organizations, and individuals. The implications of this study for our understanding of terror and future research were discussed in detail.

KEYWORDS

Cyberterrorism; far left; ecoterrorism; cybercrime; hacking; terror

This study examines the nature and scope of cyberattacks committed by ideologically motivated actors. Specifically, the study examines the methods employed by far-left groups to engage in cyberattacks and their targets. This research addresses four key gaps in the current state of knowledge related to terror and extremism. First, this study expands the terrorism literature beyond a focus on the role of computers and the Internet as a recruitment tool to understand its function as a medium for committing attacks against infrastructure. A small but growing body of research has begun to explore the intersection between terrorism and cyberspace. For instance, Weimann[1] explained that "Islamists and Marxists, nationalists and separatists, racists and anarchists: all find the Internet alluring," and that there has been an alarming and growing number of "terrorist websites." Most studies to date examine how the far right and Islamist extremists use technology as a recruitment and information tool. In fact, studies note the far right's use of technology dates back to the early 1990s when they tried to communicate secretly and recruit new members using bulletin boards and websites.[2] More recently, Islamist terrorists and extremists expanded their online

CONTACT Thomas J. Holt holtt@msu.edu School of Criminal Justice, Michigan State University, 434 Baker Hall, East Lansing, Michigan 48864, USA

present affiliation Mattisen Stonhourse Northeastern University, Boston, Massachusetts, USA

communications to include social encrypted messages on media platforms, Internet-based telephones, and dead drop email exchanges.[3] There has been far less empirical research studying the extent of computer hacking and targeted attacks against websites and online infrastructure by ideologically motivated attackers.[4]

Second, this study is among the first to investigate cyberattacks committed by far-left groups and their supporters, including the Animal Liberation Front and Earth Liberation Front, and their targets in online environments. To that end, we created and analyzed a unique database of 26 cyberattacks committed by far-left groups and affiliated actors in the US, UK, and Canada from 2000 to 2015 respectively. We used qualitative research methods to identify trends in attack methods, targets of attacks, and ideological ideas expressed through the course of an attack. The trends in cyberattacks were also compared to trends in physical attacks performed by far-left groups as identified in the Extremist Crime Database (ECDB).[5] The findings directly impact our understanding of terror, extremism, cybersecurity, and law enforcement.

Third, this study uses an innovative approach to investigate a challenging research topic area. The absence of empirical data on the nature and scope of cyberattacks associated with ideologically motivated actors is likely a function of underreporting by victims.[6] Businesses and government organizations tend not to report experiences with cyberattacks, ideologically motivated or otherwise, to the police or the general public.[7] Such attacks are also excluded from broader terrorism databases.[8] Additionally, there are currently no existing statutes for cyberterrorism within US federal criminal code. Instead, extremists committing cyberattacks are often prosecuted under existing criminal codes dealing with computer hacking.[9]

Without evidence quantifying the realities of ideologically motivated cyberattacks, some question how active extremists actually are online. Similarly, some wonder if the focus on cyberterrorism is simply a projection of the terrorism and homeland security apparatus to gain more funding and stoke public fears.[10] Finally, for the cyberattacks that are committed, we currently do not know which methods are more employed by extremists and ideologically motivated actors, who is targeted, or whether cyberattacks mirror or vary from physical attacks committed by these extremist movements. This study attempted to address these gaps in order to improve our understanding of the nature of terror and extremism both on- and off-line.

Technology use and abuse among extremists

Most previous research focuses on general issues related to extremists' use of the Internet for communication and recruitment. For example, most terrorist organizations have an Internet presence in keeping with the general rise in Internet use among the general public in Western nations. Weimann concludes, "When this research was started in the late 1990s, there were merely a dozen terrorist websites; by 2000, virtually all terrorist groups had established their presence on the Internet and in 2003 there were over 2,600 terrorist websites. The number rose dramatically and by January 2010 the archive contains over 7,600 websites serving terrorists and their supporters."[11] He also found that all organizations designated as Foreign Terrorist Organizations by the United States State Department had a website.

Similarly, research by Chermak, Freilich, and Suttmoeller compared the organizational characteristics of violent and nonviolent hate groups in the United States.[12] Their data were unique because they sampled from all hate groups—both non-violent and violent—in the United States. They found that the vast majority of hate groups involved in

ideologically motivated violence had an Internet presence. Nearly half of the organizations attempted to recruit individuals to their organization using the Internet.[13] Scholars have concluded that the Internet is often used to create a community where hate and violence are reasonable.[14] The amount and type of information provided by different types of extremist and terrorist groups on the Internet varies. This is not surprising because there is variation in the technological expertise of groups, the access an organization has to monetary resources to create and maintain a web presence, and the amount of time a group has for updating and improving the website.

Most groups' websites seek to further their movement generally, such as sites where Islamists post "cyber fatwas," promote terrorist ideologies, and explain methods to engage in violence against various targets.[15] Similarly, far-right anti-abortion activists have publicized "hit lists" online that contain names and addresses of specific physicians who have performed abortions.[16] Eco and animal rights extremists have also publicized online specific potential targets.[17]

The focus of previous research has been on general patterns in activity, and there is very little empirical work on the methods used by ideologically motivated offenders to commit cyber-attacks. The studies that have been published have used content analysis of web-related materials, such as posts in forums or on websites, as well as interviews with activist hackers. For instance, Jordan and Taylor conducted interviews with a small sample of hackers who targeted systems in support of activist agendas to consider the extent to which hacking could be used to support ideological beliefs.[18] Similarly, Woo and colleagues utilized a content analysis of 462 defaced websites to examine changes in actor behavior over time.[19] The defacements examined were motivated by various grievances, including nationalism, religion, ethnicity, and freedom of information. This study indicated that over 70 percent of the pages were hacked as a prank rather than for political motivation.[20] There were also significant differences observed in the content of defacements based on the attackers' motivations. Politically motivated hackers were significantly more likely to use aggressive expressions, including profane or obscene language. They also found that militant hackers made greater use of various communication channels, and were more likely to add photos, audio material, and hyperlinks to demonstrate their beliefs and causes.[21]

More recently, Holt, Freilich, and Chermak interviewed a small sample of Turkish hackers to understand their methods and motivations.[22] These actors reported maintaining values that reflect the beliefs of the larger hacker subculture in terms of skill development and technological understanding. At the same time, these actors reported targeting systems that reflected their ideological beliefs related to Islam and the status of Turkey in the broader world. Further, Turkish hackers reported engaging in any attack method which suited their needs at that time, though there was some evidence of preferred attack techniques which may lead to relatively tailored and consistent attack patterns over time.[23]

Differentiating actors based on ideological belief

Research on terror attacks has increased dramatically over the past two decades with a substantial focus on both etiological and counterterrorism issues, including prevention policies, associated with the Islamist and far-right threats. A few studies have examined

differences between ideological actors and the factors associated with involvement in physical acts of violence.[24]

Scholars have demonstrated that it is important to disaggregate terrorism because there are important differences across the various kinds of ideologically motivated violent extremists. In the U.S., extremists have been found to vary in terms of their age, race, gender, occupation, education, religious beliefs, where they live, and importantly, who/what they attack.[25] In response, law enforcement and security agencies have placed substantial investments in enhanced physical security measures, such as gates, barriers, screening tools, and other resources, to minimize the harm caused by a potential attack.

Research on radicals and terrorist groups demonstrates there are differences in the demographic and behavioral backgrounds of actors based on their leanings to the left or right.[26] While far-right ideologies are typically linked to nationalistic, individual-liberty based agendas supported in part by conspiratorial views, the far left highlights economic, racial, ethnic, religious, and other types of systematic injustice and oppression.[27] The far left believes that corporations, government, and other social institutions are responsible for these injustices. One part of the far left argues that animals and the earth are being irreparably harmed and must be defended by violence when necessary. Evidence suggests individuals involved in far-left acts of violence tend to be younger, may be male or female (but significantly more females are involved in such groups compared to far-right and Islamist extremist organizations), with higher levels of education and more job skills generally.[28] Additionally, they tend to operate in more urban areas and engage in more preparatory offenses prior to acts of violence.[29]

Violent far leftists also tend to report lower levels of mental illness compared to both violent far-right and Islamist extremists.[30] The ideological beliefs of the far left also lead them to target property and material resources used by corporations and organizations that directly harm the environment or biological diversity.[31] For instance, far-left actors often engage in arson or physical damage to equipment to slow construction site operations. Comparatively, the far-right and jihadist movements tend to target people more frequently than equipment or buildings.[32]

Potential use of cyberattacks by far-left groups

Based upon the far left's anti-corporation, and in some cases anti-capitalist beliefs, it is possible they may be more likely to engage in cyberattacks against ideological targets as an analog to real-world violence. The Internet is now a pivotal resource for commerce and public engagement with the world.[33] Any attack that limits customers' ability to complete a transaction may embarrass the organization's public stance and could undermine their profits. To that end, cyberattacks are increasingly targeting databases of sensitive information retained by organizations and corporations.[34] Companies typically house customer data to ensure rapid completion of financial transactions, such as the purchase of goods. Hackers motivated by financial gain frequently attempt to access this data and either use it to engage in fraudulent transactions or sell the information to others via online markets.[35]

An ideologically motivated actor could utilize the same techniques to acquire customer data and release it to the public to embarrass either the target organization or their customers.[36] Similarly, accessing sensitive personal information and posting it for public consumption could enable others with similar ideological beliefs to target individuals for

harassment on- and off-line. This phenomenon is known as "doxing," or the release of identity documents and information associated with a target.[37]

Another common tool in the arsenal of hackers seeking to express their opinion are web defacements, where the normal html code of a web page is replaced or supplemented by images, text, and content of the attacker's choosing.[38] Web defacements originally began as a method for hackers to call out system administrators who used poor security protocols to manage their website or server, and also to generate a reputation as a skilled individual in the hacker community by publicly promoting their attack.[39] Hackers still commonly employ web defacements, particularly those who are either new to the scene or interested in identifying weaknesses in servers or websites.[40]

There is also evidence that ideologically motivated hackers utilize web defacements to state their ideological beliefs to the world, and target specific institutions or entities to draw attention to their cause.[41] This sort of attack can embarrass their target due to the perception that their security protocols are weak, while creating an opportunity for attackers to express dissent or attribute the attack to a specific social cause or ideology.[42] Some attackers may also delete the original web content entirely, which may cause more harm than simply redirecting the site to a separate page.[43] The downtime an online retailer experiences while attempting to repair the damaged site may also cause economic harm for the victim.

An additional attack method that an ideologically motivated attacker may employ involves distributed denial of service (DDoS) attacks against websites and servers. A denial of service attack involves a flood of requests that are sent to webservers that overwhelms the resource, rendering them unusable to others.[44] Such attacks can cause financial harm to a target by eliminating customers' and employees' ability to use their service. In fact, recent estimates indicate that the average cost to defend a company against DDoS attacks that result in site downtime is $2.5 million.[45] DDoS attacks can be performed through the use of various tools which can be rented or obtained for free from various attacker groups on-line.[46] For instance, the hacker group Anonymous has gained attention for their use of a DDoS tool called the "Low Orbit Ion Cannon." This program has been used in attacks against personal, industrial, and government targets around the world in furtherance of their beliefs of transparency, anarchy, freedom of information, and the removal of intellectual property laws.[47]

With this in mind, it can be assumed that actors may target individuals or businesses that generally conform to a broader ideological agenda.[48] In the case of actors associated with far-left ideologies, they may be more likely to target furriers, construction companies, animal laboratories, or university researchers who use animals in their work. Such entities align with the ideological agenda of far-left groups and would often be the target of physical attacks offline. At the same time, actors may simply attack targets of convenience, as the security and vulnerability of online targets may differ substantially. Thus, actors may attempt but fail to succeed in attacks against various targets.

The method of attack may also lead to differences in the extent to which attackers can express their ideological agenda. For instance, a DDoS attack may be stealthier from an ideological perspective, as the site may be taken down, but customers may be unaware of the reason behind the attack. It is incumbent on actors to forewarn their victim or explain their motives for the attack via social media and other online outlets. By contrast, web defacements provide a prime opportunity for messaging and promotion of ideological beliefs as wide audiences can see the attackers' content when attempting to visit the site.[49]

Doxing behavior and data breaches may be similarly public in nature as the attacker must publicly post the acquired information in various online outlets.[50] It is unknown how often such incidents occur or the extent to which organizations, governments, and individuals are targeted as a result.

Data and methods

In light of the lack of empirical research on the issue of ideologically motivated cyberattacks, this study examines five key research questions:

(a) What is the prevalence of various forms of cyberattacks attributed to or claimed by far-left groups?
(b) Do cyberattacks involve single or multiple attack methods?
(c) What entities or individuals are commonly targeted in these attacks?
(d) Are the targets of cyberattacks the same types of targets attacked by real-world animal and eco-extremists bombings and arsons?
(e) To what extent do groups or individuals express ideological sentiments about their cyberattacks through statements posted online or in media outlets?

This analysis attempted to address these issues by innovatively creating one of the first databases that include a sample of cyberterrorism attacks committed by far-left extremists. We then compared these data to information on physical attacks performed by far-left groups within the Extremist Crime Database, or ECDB.[51]

Cyberattacks were identified based on purposive inclusion criteria related to the physical location of the target and the time of the attack or attacks. Specifically, cyberattacks affecting targets in the US, Canada, and the UK were selected to reflect the most prevalent potential locations for far-left groups. These nations were purposively selected due to the extent of ideological attacks and incidents attributed to far-left groups during the period of study. Additionally, the global nature of the Internet affords attackers, regardless of their location in physical space, with the ability to target resources in any country.[52] Thus, a multinational sample was developed to better reflect the borderless nature of cyberattacks generally. While data collection is ongoing, this analysis focused only on incidents occurring between the years 2000 and 2015 to capture the greatest amount of evidence on cyberattacks performed. Any attack that was included includes attacks committed by far-left groups traditionally associated with attacks in the real world.

The 26 attacks were performed by individuals and groups associated with radical far-left ideologies and/or movement groups (see Table 1 for detail). We use the ECDB's definition of far-left extremism that characterizes animal and environmental rights movements and organizations that support violence and crime to defend the earth from corporations and governments that mean it harm.[53] In particular, this study captured attacks performed by the Animal Liberation Front, Earth Liberation Front, and individuals espousing similar ideological beliefs. Animal Liberation Front (ALF) identifies itself as an organization that takes illegal actions against industries profiting from animal exploitation. ALF's operations follow a set of strict guidelines: to cause economic harm to those profiting from the exploitation of animals; to engage in nonviolent actions and liberations to raise awareness of malicious behaviors against animals; and to take the needed

Table 1. The Distribution of Attack Types within This Sample

Incident #	Date of Attack	Group Affiliation of Attackers ALF	Anonymous	ELF	Other	Total
1	07-03-2007	1	0	0	0	1
2	1/19/2009	1	0	0	0	1
3	3/13/2009	1	0	0	0	1
4	7/23/2010	0	0	1	1	2
5	07-12-2011	0	1	0	0	1
6	10-01-2011	1	1	0	0	2
7	11/15/2011	0	0	0	1	1
8	3/19/2012	1	0	0	0	1
9	06-06-2012	0	1	0	0	1
10	06-07-2012	0	1	0	0	1
11	08-10-2012	1	0	0	0	1
12	8/27/2012	0	1	0	0	1
13	03-05-2013	0	1	0	0	1
14	4/24/2013	1	0	0	0	1
15	06-10-2013	1	0	0	0	1
16	01-01-2014	0	1	0	0	1
17	04-05-2014	1	0	0	0	1
18	10-02-2014	0	0	0	1	1
19	10/13/2014	1	0	0	0	1
20	11/30/2014	0	0	1	1	2
21	04-01-2015	0	1	0	0	1
22	4/26/2015	0	1	0	0	1
23	09-07-2015	1	0	0	0	1
24	10/28/2015	0	1	0	0	1
25	10/28/2015	0	1	0	0	1
26	12/22/2015	0	1	0	0	1
Total		11	12	2	4	29

precautions to prevent the harming of all animals, humans, and non-humans. Earth Liberation Front (ELF) is an environmental movement without central leadership. The organization began in 1992, stemming from the collective Environmental Life First. ELF operates as an eco-guerrilla combat unit fighting the exploitation of the environment.

This study also included attacks performed by the hacker collective Anonymous, which originated from the board 4chan, where individuals began to share images without revealing personal information about themselves. As individuals continued to post pictures without identifying themselves, it led to the popularity of the idea of Anonymous being a real person.[54] Anonymous became a collective identity surrounding the idea of the Internet being an outlet without limits or boundaries. They have no specific ideological leaning, and instead engage in attacks against any target based on the broader interests of any part of the collective.[55]

It should be noted that attackers noted their ideological affiliations, which in some cases included different groups working in tandem to complete an attack. While this is relatively uncommon in physical attacks, there were several instances of groups working in concert

Table 2. Incident Details and Attacker Affiliations

Incident #	Media Accounts	Watch Groups	Offender Self-Report	Social Media	Other Sources	Total Total
1	0	3	1	0	1	10
2	1	0	1	0	2	4
3	0	0	6	0	1	7
4	5	3	3	0	1	12
5	3	6	6	3	3	21
6	0	1	0	2	1	4
7	20	9	0	0	13	42
8	0	0	0	0	2	2
9	1	1	4	2	1	9
10	1	0	2	1	2	6
11	0	0	1	0	4	5
12	1	0	4	2	2	9
13	2	0	1	0	1	4
14	9	1	1	0	5	16
15	3	1	2	0	3	9
16	2	0	1	1	0	4
17	0	0	0	0	4	4
18	27	6	0	0	11	44
19	0	0	0	0	2	2
20	4	0	0	0	1	5
21	6	1	1	2	2	12
22	3	0	4	2	0	9
23	0	0	1	0	5	6
24	0	1	1	0	1	3
25	5	5	1	2	4	17
26	1	0	1	2	1	5
Total	97	36	41	20	77	271

during cyberattacks. These instances are highlighted to demonstrate connections between groups.

The initial sample of attacks were generated through web searches in Google and Bing using terminology such as *animal liberation front hack, earth liberation front hack*, and *cyberattack*. Details regarding the attacks were collected from five primary source types, mirroring that of the ECDB and other open-source terrorism databases: a) media sources, b) watch groups, c) offender self-reporting through websites, d) social media sources, and e) other content sources (see Table 2 for details). The majority of information was produced from media outlets (35.8%) and other sources (28.4%), which included Pastebin sites where offenders may have placed data, as well as academic reports and research works. Importantly, 15.1% of the content for this analysis was also generated from the offenders via web spaces they operate. Thus, ideological actors appeared to take some steps to claim responsibility for cyberattacks on behalf of their group or belief system,[56] similar to claims made in physical attacks through press releases by responsible groups.[57]

These sources were used to triangulate information about the attack method, the target, and actors involved. Data documented about the attack included the date of the incident, the news media, if any, that reported the cyberattack, whether the incident was reported to

Table 3. Data Sources by Incident

Incident #	Data Breach	Defacement	DOS	DOX	Total
1	1	1	0	0	2
2	0	0	1	0	1
3	0	0	1	0	1
4	0	1	0	0	1
5	1	0	1	1	3
6	1	1	0	0	2
7	1	0	0	0	1
8	1	0	0	0	1
9	1	0	0	0	1
10	1	0	0	1	2
11	0	1	0	0	1
12	1	0	0	1	2
13	1	0	0	0	1
14	1	1	0	1	3
15	1	0	0	0	1
16	0	0	0	1	1
17	1	1	0	0	2
18	0	0	1	0	1
19	1	0	0	1	2
20	0	1	0	0	1
21	0	1	1	0	2
22	0	0	1	0	1
23	0	1	0	0	1
24	1	0	0	0	1
25	1	0	0	0	1
26	1	1	0	1	3
Total	16	10	6	7	39

authorities, and the attack method used. This information also included the outcome of the attack, the impact and economic cost, and whether the attack had been successful. Information on actors consisted of group affiliation, the actor's attribution, the perpetrator's real name, whether they were caught by officials, and the motive of their attack. Details on targets included the location of the victim, the type of company, and their name. The target data also encompassed the target type (e.g., business, government, military), the number of targets involved in the attack, and whether there had been direct communication between the victim and authorities afterwards.

Attack trends could be observed through various lenses such as the group affiliation, attack method used, and motivations behind the attack. The cyberattacks documented in the study were categorized into four different attack methods based on prior research related to cyberattacks (see Table 3).[58] Data breaches were the first category included, defined as the illicit acquisition and possible release of sensitive personal information. Defacements were the second category, reflecting any attack performed by individuals to remove and replace the content of a website. The third category, denial of service (DoS) attacks, reflects the use of tools or techniques to flood a website or server with requests to render it useless. The final category included doxing incidents, where individuals' private

material is posted online with the intent to cause harm to the victims. Within the 26 incidents examined, the majority involved only a single form of attack (n = 16; 61.5%). The remaining ten incidents involving multiple attacks will be discussed in detail.

Due to the qualitative case study method employed in this analysis, quotes from the data will be presented where appropriate to illustrate the attackers' behaviors, victims' views or responses to the incident, or ideological expressions made before, during, or after the incident. Each form of attack will be discussed separately, though instances when multiple attack methods were employed will be discussed when appropriate to highlight overlapping methods or outcomes against a specific target.

To assess any similarities between cyberattacks and physical attacks, we extracted all real-world animal and eco-extremist attacks from the ECDB. The ECDB is an open-source database that includes bombings and arsons committed by individuals affiliated with ELF or ALF who were convicted between the years 1995 and 2015.[59] A full summary of the data collection methodology for the real-world attacks can be found in the article, "Introducing the ECDB."[60] It must be noted that the ECDB currently includes attacks occurring only within the United States, thus the potential universe of physical incidents differs slightly from that of the cyberattack data. At the same time, the extent of physical attacks still provides a useful point of comparison against cyberattacks generally.

Attack details

The data collected in this analysis suggest that there has been a substantive increase in the number of cyberattacks performed since 2011. There were no attacks identified affecting Canada, the UK, or US between 2000 and 2006, and increases in incidents were inconsistent year after year until 2011 (see Table 4 for details). The majority of attacks occurred in 2012, 2014, and 2015 respectively. Data breaches were the most common attack

Table 4. Cyber and Physical Attacks by Year

Year	Attack Method Data Breach	Defacement	DOS	DOX	Total	Physical Attack
2000	0	0	0	0	0	18
2001	0	0	0	0	0	22
2002	0	0	0	0	0	9
2003	0	0	0	0	0	27
2004	0	0	0	0	0	17
2005	0	0	0	0	0	18
2006	0	0	0	0	0	4
2007	1	1	0	0	2	10
2008	0	0	0	0	0	18
2009	0	0	2	0	2	3
2010	0	1	0	0	1	10
2011	3	1	1	1	6	2
2012	4	1	0	2	7	2
2013	3	1	0	1	5	0
2014	2	2	1	2	7	0
2015	3	3	2	1	9	1
Totals	16	10	6	7	39	161

method, though they varied in their use year over year beginning in 2011. Website defacements were the most consistent, with an attack reported every year from 2010 to 2015. Data doxing occurred with some consistency from 2011 to 2015, while DDOS attacks varied from year to year. These trends do not appear to mirror that of broader cybercrime trends, with the exception of data breaches, which have increased substantially over the last decade.[61]

Comparing cyberattacks to physical attacks reveals an interesting trend. Physical attacks were much more common in the early to mid-2000s. There was, however, a substantial decline in physical attacks noted within the ECDB beginning in 2009, which continued through the first half of this decade. The number of cyberattacks concurrently rose during this period, suggesting a potential shift in the practices of far-left attackers. It is not clear what factors may account for this trend, though it highlights the growing importance of cyberattacks for activists and ideologically motivated actors generally.[62]

The majority of attacks were performed by Anonymous (46.5%; see Table 5). This may be sensible as Anonymous is largely thought to have no specific orthodoxy or ideological agenda, though they have historically targeted large organizations, security corporations, businesses, and law enforcement.[63] As a result, they may be more like anarchists who are generally left-leaning from an ideological perspective. In addition, Anonymous almost exclusively engages in cyberattacks and hacks, which may make their members more capable of completing such attacks relative to ALF or ELF, which tend to act in physical space.

Anonymous attacks observed in this sample fit within broader trends identified in their general cyberattack campaigns. Anonymous primarily engaged in data breaches (45%) and doxing incidents (25%), and performed half of all denial of service attacks within the overall sample. At the same time, ALF attackers were the second most prevalent overall (n = 17; 39.5%), with the majority of their attacks involving data breaches (41%) and web defacements (35%), while only two attacks were attributed to ELF (4.7%) during the period of study. The attacks within the other category (9.3%) include either individuals or attacks associated with groups tied to an ideological agenda, such as PETA.

Table 6 compares the targets of both cyberattacks and real-world attacks. All of the real-world targets were attacked by either arson or bombings. Examining the cyber-targets of attacks demonstrated most groups targeted businesses, particularly medium (19.3%) and large organizations (35.4%; see Table 5). Attacks against large businesses were performed by all four far-left groups in this sample, with the majority performed by ALF and Anonymous. The majority of attacks against businesses, regardless of size, were performed by ALF-associated attackers (45% overall). A small number of government resources were also targeted (16.1%), with those attacks stemming mostly from Anonymous-affiliated actors (80%).

Table 5. Attacks Segmented By Ideology

Attack Type	Ideology ALF	Anon	ELF	Other	Total
Data breach	7	9	0	1	17
Defacement	6	3	2	2	13
DOS	2	3	0	1	6
DOX	2	5	0	0	7
Total	17	20	2	4	43

The targets affected by real-world attacks were quite similar to those of cyberattacks, with two exceptions: construction vehicles (17.5%) and homes (17.7%). Despite this difference, the majority of attacks targeted businesses, particularly if construction equipment was included in this category. Medium businesses were the most common target overall (35.2%), while small businesses (8.6%) and large businesses (7.1%) were less common. Attacks against educational institutions accounted for a smaller proportion of cyberattacks compared to physical attacks (8.9%). Similarly, government targets were affected by cyberattacks (16.2%) more often than physical attacks within this period (2.7%).

Comparing targets by attack type demonstrated that multiple targets could be affected by attacks in any incident (see Table 7), which is why there are more targets affected by attacks than identified in Table 3. In addition, the majority of attacks affecting all businesses involved some type of data breach (52.6%), leading to the release of customer or employee data. The majority of breaches (37.5%) affected large businesses, which is sensible given their involvement in various practices that draw the ire of far-left groups, such as harming the environment or animals. In some cases, these breaches also led to doxing incidents as the information released could be used to identify individual customers or employees. The federal government was also primarily affected by data breaches (60%), though when combined, federal and state/local websites were frequently targeted by denial of service attacks (42.8%). Individuals were also targeted by data breaches (50%), while the websites and entities in the other category were primarily impacted by defacements (60%).

Data breaches

Examining the individual forms of attack provides greater insights into the nature of ideological cyberattacks. Data breaches were the most common attack observed in this sample, with 16 of the 39 (41%) cyberattacks involving illicit access to personal data (see Table 3 for details). The attacks were claimed by Anonymous and Animal Liberation Front actors. A variety of industrial and government-related entities were targeted, including the US Department of Agriculture, the local Hawaiian government, the Intel corporation, mining and oil companies, animal laboratories, and two small businesses (see

Table 6. Targets Attacked By Ideological Group

	Ideological Affiliation					
Target	ALF	Anonymous	ELF	Other	Total	Real World
Business, Small	2	1	0	0	3 (9.7%)	35 (8.6%)
Business, Medium	3	1	1	1	6 (19.4%)	143 (35.2%)
Business, Large	4	4	1	2	11(35.5%)	29 (7.1%)
Educational Institution	1	0	0	0	1 (3.2%)	36 (8.9%)
Government, Federal	0	3	0	0	3 (9.7%)	6 (1.5%)
Government, State/Local	0	1	0	1	2 (6.5%)	5 (1.2%)
Individuals	0	1	0	1	2 (6.5%)	9 (2.2%)
Construction Vehicles/Cars	0	0	0	0	0 (0.0%)	71 (17.5%)
Homes	0	0	0	0	0 (0.0%)	72 (17.7%)
Other	2	1	0	0	3 (9.7%)	0 (0.0%)
Total	12	12	2	5	31 (100%)	406 (100%)

Table 4 for details). Information lost in the breaches was composed of usernames, passwords, phone numbers, home addresses, and other personal data belonging to employees, clients, customers, investors, and shareholders. These attacks sought to protest or retaliate against organizations or companies the actors felt did not align with their ideologies.

While data breaches are traditionally associated with economic loss when targeting financial institutions and retailers,[64] it is unclear what, if any, economic repercussions were experienced by victims as a result of the data loss. There was also no immediate evidence to suggest the corporate and government targets experienced any reputational damage as a result of the breaches. For instance, members of the hacker collective Anonymous compromised the US National Agriculture Library, a part of the US Department of Agriculture, in October 2015. The attackers were able to acquire a database of staff, clients, contractors, and related individuals associated with the NAL, including usernames and passwords for internal systems. The group posted this information online, and when interviewed by a journalist indicated they performed the attack "based on their affiliation with big fishes we op [target] against. We will fight Monsanto and its poisonous food products."[65]

Similar actions were observed in one of the ALF breaches targeting UK-based badger hunting groups. The attackers appeared to utilize some sort of phishing attack in order to gain access to sensitive information on the operators and their clients. The ALF reported this attack on their website, noting:

> [the company's] security is so poor. All it took was for them to be contacted by 'Bill from Microsoft' and within no time at all they had downloaded the 'bug fix', given us their passwords and were asking for tips on how to use word! We are now able to download contact and bank account details of suppliers and clients and even scans of shotgun licences. Some of these files show deliberate attempts to avoid paying VAT (sales tax).

The attackers also released customers' personal information in a data file that was publicly available for download online in order to embarrass them for their patronage.

A similar attack was performed against a "foie gras" producer, which is the French name for goose or duck liver that has been fattened by force feeding the animals. The attackers posted the following information on the Animal Liberation Front website:

Table 7. Targets Attacked By Attack Type

Target	Attack Type Data Breach	Defacement	DOS	DOX	Total
Business, Small	2	1	0	2	5
Business, Medium	2	2	1	0	5
Business, Large	6	3	2	3	14
Educational Institution	0	1	0	0	1
Government, Federal	3	0	1	1	5
Government, State/Local	0	0	2	0	2
Individuals	2	1	0	1	4
Other	1	3	1	0	5
Total	16	11	7	7	41

> For Earth Day we targeted Hudson Valley Foie Gras, the largest foie gras farm in the United States. Hudson Valley Foie Gras tortures birds and pollutes the earth. The company has been fined tens of thousands of dollars for violations of the Clean Water Act. We temporarily took down their website (www.hudsonvalleyfoiegras.com) and online store, and uncovered name/address/phone number/credit card details for over 1,200 customers who purchased foie gras and duck flesh products between June 2012 and April 2013… . The customer list includes many in California, where the production and sale of foie gras is illegal.

The attackers then doxed, or listed, the names and email addresses of customers and attempted to embarrass specific customers by indicating how much product they purchased on what day using a specific credit card. They used specific language stating: "On 3/27/2013, [victim name] used his American Express card to buy $351 worth of foie gras. On 2/5/2013, [victim name] charged $686 worth of dead duck to his MasterCard. On 12/5/2012, [victim name] used her American Express card to buy $1,103 worth of "Fresh Foie Gras."

A representative for the victim company was interviewed about the hack, and seemed relatively unconcerned over the incident:

> Our farm has been broken into numerous times over the years, equipment damaged, and there are the lawsuits that are filed against us, so this is an ongoing thing. We've never had our website hacked, but it's all part of the same set of attacks against our farming practices. And hey if the AP can get hacked, I'm sorry but it's just something that happens.

The parity noted between physical and cyberattacks that the company has experienced in the past suggest that it may be expected given the nature of their product and the outrage it produces among the animal rights community.

Defacements

Ten of the incidents in the study (26%) involved website defacements, though they were performed either by a single group or actors collaborating across groups. Additionally, one actor engaged in a defacement and claimed to be affiliated with People for the Ethical Treatment of Animals (PETA). The defacement targets ranged from furrier companies to animal research institutes and laboratories. The primary motivations behind these attacks were to raise awareness of various issues or protest an organization, as evident in the language used within the defacements themselves. For instance, an attacker defaced a small business's website and compromised their customers' data and posted it online. In the defacement, the attacker posted the customer information along with the following message:

> To the owners of 'The twisted pine fur and leather company' you have no excuse to sale [SIC] the flesh, skin and fur of another creature. Your website lacks security. To the customers, you have no right to buy the flesh, skin or fur of another creature. You deserve this. You're lucky this is the only data we dumped. Exploiters, you've been warned. Expect us.

A similar attack was observed against another furrier, and the defacement included pictures of live animals and an apology to the system's administrator, noting:

> I did not hack this site in order to cause trouble for anyone (except maybe [the company]). I fully understand the responsibilities [SIC] of a system administrator and understand it is a thankless job. This is in no way the administrator's fault (or whoever is in control of security at [name removed]). I tried to do this as carefully as I could, in order not to cause any problems for the site administrator(s). Anyway, this was done in the name of animal rights.

Today's consumer is completely oblivious to what goes on in order for their product to arrive at the mall for them to buy. It is time that the consumer be aware of what goes on in many of today's big industries. Most importantly, the food industries. For instance, dairy cows are injected with a chemical called BGH that is very harmful to both humans and the cows. This chemical gives the cows bladder infections. This makes the cows bleed and guess what? It goes straight in to your bowl of cereal. Little does the consumer know, nor care. The same kind of thing goes on behind the back of fur wearers. The chemicals that are used to process and produce the fur are extremely bad for our earth. Not only that, but millions of animals are slaughtered for fur and leather coats. I did this in order to wake up the blind consumers of today. Know the facts.

These attacks indicate the differing motives of far-left ideological extremists. In some cases, the actors would attack organizations in protest, wanting to cause damage to their targets. In other cases, the attackers sought to raise awareness to an organization's consumers, not focusing on harming the organization itself. In certain instances, attackers wanted to harm companies while also raising awareness of the companies' practices. For example, one attacker defaced a dogfighting smartphone app website, and then hacked the application itself, installing malicious software within the program. Once the application was opened, it would access the smartphone contact list and send a text message to every available number stating: "I take pleasure in hurting small animals, just thought you should know that." The malicious code also automatically signed up users for a PETA text messaging service. In this case, the actors wanted not only to deface the dogfighting app, but to shame individuals for using it.

An additional defacement associated with the ALF-affiliated hacker group, PwnedSecurity Team Canada, targeted the website of an organization promoting humane animal research in the UK. When the attackers gained access to the site, they not only defaced the site, but also adjusted the existing files hosted online. The attacker noted:

> There is a section of the website with a number of pdf files for visitors to download. We replaced all of this big pharma funded propaganda with pdfs from the Physicians Committee for Responsible Medicine (PCRM) explaining the scientific flaws with animal testing. These have now been on the website for quite some time. Until UAR fix[es] the several security holes we found in their website you can see the replacement pdfs by visiting http://www.animalrightsextremism.info/resources/documents and clicking any of the links. We did a few other even less obvious things to the site besides replacing the pdfs but it will be amusing to let UAR try to find everything for themselves without being told what to look for.

Thus, defacements provided unique and overt insights into the practices and beliefs of ideological attackers operating in online spaces.

Denial of service attacks

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks made up six of the incidents in the study (15%). Three of these were conducted by Anonymous, two were performed by ALF-associated attackers, and one was performed by an individual. Specifically, a DoS attack was conducted by a 15-year-old boy and his unknown partner with the screenname "Whitehat," targeting SeaWorld and the Devon and Cornwall Police. Although no information could be found to account for his attack against the police, the

boy claimed to be an animal rights activist. His attack on SeaWorld was thought to have cost the company approximately $500,000 in lost revenue while the site was down.

DDoS attacks tended to have less ideological information associated with the incidents, save for the actors claiming responsibility for the attacks. One of the more substantial ALF-associated attacks targeted Huntingdon Life Sciences, a laboratory based out of the United Kingdom and known for using animals in its biomedical and pharmaceutical research. Similarly, one of the attacks performed by an Anonymous-associated group targeted a Hawaiian government website for their involvement with Thirty Meter Telescope (TMT). The organization has installed 13 telescopes on Mauna Kea, which had been protested in physical spaces by native Hawaiian groups on the basis that the mountain was a sacred site that should not be disturbed.

The incident was reported on a blog called "Operation Green Rights," which provided details on their attacks and communications, as well as a Twitter account where Anonymous claimed responsibility. The attackers were able to successfully take the telescope's website offline for two hours, and affected the state government's website for at least seven hours. Anonymous posted multiple messages on twitter associated with the attack, one of which stated: "nothing will ever justify the destruction of ecosystems; filthy money can never replace them."[66] A different post included a screenshot of the downed government website along with the message: "#DDoS against site of #Hawaii government portal.ehawaii.gov STOP ecocide and native rights abuses #WeAreMaunaKea."[67]

Doxing

Seven of the incidents in this sample involved doxing (18%), the majority of which were performed by groups or individuals associated with Anonymous (71.4%). These incidents were partially associated with data breaches, as described above, though some of the attacks also targeted single individuals for their role in specific incidents or events. All of these attacks were also designed to draw public attention to a problem, while simultaneously publicly shaming the targets and enabling the broader population of Internet users to harass or threaten them.

The targets of the doxing cases varied, ranging from a single individual to thousands depending on the target and the incident that spawned the attack. For instance, #OpFunKill was an attack against the Dallas Safari Club after they auctioned off a license to kill an endangered black rhino in Namibia. The hunter who won the auction, Corey Knowlton, paid $350,000 for the license. Anonymous attacked the Dallas Safari Club website and members that participated in the auction. Knowlton was doxed, his name and personal information leaked online, and shortly thereafter he began to receive death threats. Similarly, a taxidermist named Debbie Byrd was doxed after she shared a picture of herself with a dead tiger on Facebook. Anonymous posted her personal information online with the intent of drawing attention to their cause. The actors accused her of murdering a healthy tiger for sport instead of showing mercy to an ill, elderly animal as she had originally claimed.

Discussion and conclusions

Although research on terrorism and cyberattacks has increased dramatically over the last two decades, there have been few empirical studies that consider the intersection of these offenses.[68] Anecdotal evidence demonstrates that ideological actors and extremist groups

are interested in utilizing computer hacks and cyberattacks to cause economic and social harm.[69] Statistics and information on the frequency and nature of ideological cyberattacks are not, however, captured in current terrorism and extremist crime data sources. To address this gap in the literature, this study utilized an open-source qualitative case study design to identify and analyze cyberattacks performed by far-left ideological groups between 2000 and 2015.

The 26 incidents examined demonstrated that far-left cyberattacks have increased over time, particularly from 2010 to 2015. The observed increase in cyberattacks coincides with the substantial decrease in physical attacks captured in the ECDB. Though several have noted the decline of physical incidents by far-left groups,[70] virtually no one predicted growth in online attacks.[71] It is unclear if the increase is a result of offenders displacing to online settings, or a form of innovation in actor or movement decision-making. It is clear that there is a reduced risk of detection and arrest for online actions. It is possible that the far left adapted to the changing opportunity structure by increasing its illegal activities online where risk is reduced, while decreasing its real-world crimes which receive more official attention and have an increased risk of detection.[72] Thus additional research is needed to systematically explore the changing patterns of action and their persistence over time.

It is also notable that the majority of these incidents were performed by individuals associated with the hacker collective Anonymous, which does not otherwise engage in attacks and behaviors commonly associated with the far left in offline spaces. At the same time, their broader targets and expressed motives for attack fit within a pattern of organizations and entities that in some way wrong society or marginalized groups.[73] Thus, future research would benefit from a deeper examination of attacks associated with Anonymous to better document the threat they pose and better map their ideological agenda to existing knowledge of terror and extremist groups.

Attacks attributed to the Animal Liberation Front were the second most common overall, and they tended to target the same entities in on-line spaces as they do off-line: furriers, retailers, corporations, and government agencies.[74] By attacking these companies and organizations, actors were able to feel as though they were fighting the injustices against animals and the environment. In this respect, it appears that cyberattacks have a similar expressive objective to physical attacks, though the economic and physical harm that may result can differ.[75]

Attackers frequently sought to either damage the reputation of their target or promote awareness of an issue to the public. The preponderance of data breaches to leak sensitive information without necessarily leading to identity theft or associated fraud reinforced the notion that these attacks were performed for an ideological, rather than economic, motive.[76] The prevalence of web defacements and their ideological messaging further supported the desire of attackers to shame companies or consumers, and draw attention to their ideological causes.[77]

Analyzing the content of the messages left by attackers demonstrated that they expressed both ideological sentiments and their assessments of the cybersecurity postures of their victims. Their comments appear to reflect combined awareness of values from both far-left groups and the broader hacker subculture as a whole.[78] The notion of poor security was particularly evident in defacements and data breaches, where attackers could apply more novel hacking techniques in order to complete their objectives.

Taken as a whole, this study suggests the threat of ideologically motivated cyberattacks cannot be ignored, nor should they be downplayed as unrealistic or non-existent.[79] Actors aligned with far-left ideologies have the skills necessary to perform cyberattacks that directly compromise personally identifiable information and security protocols. In this respect, the

methods employed by attackers do not appear to differ from that of other hackers driven by financial or status-based motives.[80] Additionally, the attacks appear to target companies and organizations that are traditionally affected by economically motivated hackers. Though the incidents did not appear to produce severe economic impacts to consumers or industrial targets, they clearly affected business operations and created costs to improve security protocols. It is also possible that victims whose personal or financial information was posted online may have experienced psychological or economic ramifications similar to that of traditional identity theft.[81] Thus, it is vital to identify potential methods for proactive actor motivation detection by cybersecurity professionals based on actor behavior during and after the incident is complete to better defend against future attacks and minimize harms.[82]

There are several limitations with the current project that highlight opportunities for additional research. First, although open-source research methodologies and strategies are still being developed, there are several potential sources of bias. The sample of events was not randomly selected, but was focused on events that occurred during a specific time frame. Additionally, the sample size is small, and may not reflect all cyberattacks committed by actors aligned with far-left ideologies.

In addition, the approach used here mirrors previously vetted and proven data collection strategies to identify open source reports.[83] At the same time, it is plausible that not all cyberattacks would become known to the public. Many cyberattack victims are afraid to report the incident due to the reputational harm it may cause, or that they were victimized depending on the nature of the attack.[84] Failed attacks may also not be recognized or discussed in open sources due to difficulties determining why an incident took place. Thus, it may be that events discussed in open sources are the most serious and successful to have occurred, limiting our knowledge of other incidents.

This analysis thus underscores the need for better data collection and statistical analysis of ideological incidents that occur in online spaces. Though this study focused on far-left attacks, there is evidence that actors on the far right and extremist Islamist communities are interested in and have encouraged cyberattacks.[85] There are multiple terrorism and extremist offender data sources that catalogue criminal incidents performed by ideologically motivated actors around the world.[86] These data sets do not incorporate measures for cyberattacks, nor do law enforcement agencies, creating the potential for ideologically motivated cyberattacks to be a truly dark figure of crime.

As a result, there is a need for dedicated data collection efforts to document the extent of these attacks, their targets, and any demographic and background information on attackers. A clear limitation of this analysis is that little information could be obtained about attackers beyond their online "handle" or ideological affiliation. Additionally, only one incident in this sample led to an arrest: a 15-year-old male who allegedly launched DDoS attacks against companies in the US and UK due to his animal rights beliefs. It is unknown how many of these attacks were facilitated by individuals or groups, and the extent of ideological ties between the attacker and the group which claimed responsibility. Such information is vital to understand whether cyberattackers could be viewed as loners, lone wolves, or are more group based, and to identify differences in organizational dynamics based on attack types.

Additional data is also needed to understand the radicalization process of cyberattackers, and any commonalities they may have with real-world violent actors. From this analysis, it appears that many of these attacks required a degree of technical skill to be successfully completed. The attackers also utilized jargon from the hacker community when describing

their actions via web defacements or claims on social media. It is unclear if the attackers developed their capacity as hackers first and then came to accept an ideological agenda later, or if they always had ideological beliefs and developed technological skills to act on those ideas.[87] Such research will require the use of novel data collection methods, particularly qualitative interviews with ideologically leaning hackers and extremist group members to develop a robust sample of actors.[88] The insights that may be gleaned could be essential to improve our understanding of the nature of terrorism and extremist threats on- and off-line. Such information could also be used to develop crime scripts and knowledge to form evidence-based defensive strategies to prevent future cyberattacks from occurring.[89]

Disclosure statement

No potential conflict of interest was reported by the authors.

Notes on contributors

Thomas J. Holt is a Professor in the School of Criminal Justice at Michigan State University. His work examines cybercrime, cyberterrorism, and the policy response to these phenomena. Dr. Holt has published his research in a range of journals including British Journal of Criminology, Crime and Delinquency, Deviant Behavior, and Terrorism and Political Violence. His work has been funded by the Department of Homeland Security, the National Institute of Justice and the National Science Foundation.

Mattisen Stonhouse is pursuing her masters' degree in cybersecurity at Northeastern University. She received her bachelors degree in criminal justice from Michigan State University in 2018.

Joshua D. Freilich is a member of the Criminal Justice Department and the Criminal Justice Ph.D. Program at John Jay College. He is the Creator and co-Director of the United States Extremist Crime Database, an open source relational database of violent and financial crimes committed by political extremists in the United States. Professor Freilich's research has been funded by the Department of Homeland Security and the National Institute of Justice. His research focuses on the causes of and responses to terrorism, bias crimes, measurement issues, and criminology theory, especially environmental criminology and crime prevention.

Steven M. Chermak is a Professor in the School of Criminal Justice at the Michigan State University, an investigator for the National Consortium for the Study of Terrorism and Responses to Terrorism, and Creator and co-Director of the United States Extremist Crime Database. He studies domestic terrorism, media coverage of crime and justice issues, and the effectiveness of specific policing strategies. Recent publications have appeared in Terrorism and Political Violence, Crime and Delinquency, and the Journal of Quantitative Criminology.

Notes

1 Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington, DC: US Institute of Peace Press, 2006), 624.

2 Steven M. Chermak, *Searching for a Demon: The Media Construction of the Militia Movement* (Boston, MA: UPNE, 2002); Jessica Eve Stern, "Weapons of Mass Impact: A Growing and Worrisome Danger," *Politics and the Life Sciences* 15, no. 2 (1996): 222–25; Michael Whine, "The Use of the Internet by Far Right Extremists," *Cybercrime: Law, Security and Privacy in the Information Age*, ed. B. D. Loader and D. Thomas (New York, NY: Routledge, 2000), 234–50.

3 Thomas J. Holt, "Exploring the Intersections of Technology, Crime, and Terror," *Terrorism and Political Violence* 24, no. 2 (2012): 337–54; Gabriel Weimann, "Cyber-Fatwas and Terrorism," *Studies in Conflict & Terrorism* 34, no. 10 (2011): 765–81.
4 Tim Jordan and Paul A. Taylor, *Hacktivism and Cyberwars: Rebels with a Cause*? (New York: Routledge, 2004); Hyung-jin Woo, Yeora Kim, and Joseph Dominick, "Hackers: Militants or Merry Pranksters? A Content Analysis of Defaced Web Pages," *Media Psychology* 6, no. 1 (2004).
5 Joshua D. Freilich, Steven M. Chermak, Roberta Belli, Jeffrey A. Gruenewald, and William S. Parkin, "Introducing the United States Extremist Crime Database (ECDB)," *Terrorism and Political Violence* 26, no. 2 (2014): 372–84.
6 Marjie T. Britz, "Terrorism and Technology: Operationalizing Cyberterrorism and Identifying Concepts," in Tom Holt, ed., *Crime Online* (Charlotte: Carolina University Press, 2012); Thomas J. Holt, Olga Smirnova, and Yi-Ting Chua, *Data Thieves in Action: Examining the International Market for Stolen Personal Information* (New York: Palgrave Macmillan, 2016).
7 Britz (see note 6); Thomas J. Holt and Adam M. Bossler, *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses* (New York: Routledge, 2016); David S. Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Cambridge, UK: Polity Press, 2007).
8 Freilich, Chermak, Belli, Gruenewald, and Parkin (see note 5); Gary LaFree, Laura Dugan, and Erin Miller, *Putting Terrorism in Context: Lessons from the Global Terrorism Database* (London: Routledge, 2015).
9 Holt and Bossler (see note 7).
10 Majid Yar, *Cybercrime and Society* (Thousand Oaks, CA: Sage, 2013).
11 Ibid.
12 Steven Chermak, Joshua Freilich, and Michael Suttmoeller, "The Organizational Dynamics of Far-right Hate Groups in the United States: Comparing Violent and Nonviolent Organizations," *Studies in Conflict & Terrorism* 36, no. 3 (2013): 193–218.
13 Ibid.
14 Josh Adams and Vincent J. Roscigno, "White Supremacists, Oppositional Culture, and the World Wide Web," *Social Forces* 84, no. 2 (2005): 759–78; Christopher Brown, "White Supremacist Discourse on the Internet and the Construction of Whiteness Ideology," *The Howard Journal of Communications* 20, no. 2 (2009): 189–208, www.hate.com.
15 Britz (see note 6); Holt (see note 3); Weimann (see note 3).
16 Chermak, Freilich, and Suttmoeller (see note 13).
17 Brent L. Smith and Kelly R. Damphousse, "Patterns of Precursor Behaviors in the Life Span of a US Environmental Terrorist Group," *Criminology & Public Policy* 8, no. 3 (2009): 475–96.
18 Jordan and Taylor (see note 4).
19 Ibid.; Woo et al. (see note 4).
20 Ibid.
21 Ibid.
22 Thomas J. Holt, Joshua D. Freilich, and Steven M. Chermak, "Exploring the Subculture of Ideologically Motivated Cyber-Attackers," *Journal of Contemporary Criminal Justice* 33, no. 3 (2017): 212–33.
23 Ibid.
24 Freilich, Chermak, Belli, Gruenewald, and Parkin (see note 5); Joshua D. Freilich, Steven M. Chermak, and Jeffrey A. Gruenewald, "The Future of Terrorism Research: A Review Essay," *International Journal of Comparative and Applied Criminal Justice* 39, no. 4 (2015): 353–69; Mark S. Hamm,*Terrorism as Crime: From Oklahoma City to Al-Qaeda and Beyond* (New York, NY: New York University Press, 2007); Gary LaFree and Bianca E. Bersani, "County-Level Correlates of Terrorist Attacks in the United States," *Criminology & Public Policy* 13, no. 3 (2014): 455–81; Gary LaFree and Laura Dugan, "Introducing the Global Terrorism Database," *Terrorism and Political Violence* 19, no. 2 (2007): 181–204; LaFree (see note 8); Smith and Damphousse (see note 18).

25 Steven M. Chermak and Jeffrey A. Gruenewald, "Laying a Foundation for the Criminological Examination of Right-Wing, Left-Wing, and Al Qaeda-Inspired Extremism in the United States," *Terrorism and Political Violence* 27, no. 1 (2015): 133–59; Jeffrey S. Handler, "Socioeconomic Profile of an American Terrorist: 1960s and 1970s," *Terrorism* 13, no. 3 (1990): 195–213; Christopher Hewitt, *Understanding Terrorism in America* (London: Routledge, 2003); Smith and Damphousse (see note 18).
26 Chermak and Gruenewald (see note 26).
27 Smith and Damphousse (see note 18).
28 Chermak and Gruenewald (see note 26); Handler (see note 26); Hewitt (see note 26); Smith and Damphousse (see note 18).
29 Ibid.
30 Chermak and Gruenewald (see note 26).
31 Ibid.
32 Ibid.
33 Susan W. Brenner, *Cybercrime: Criminal Threats from Cyberspace* (Santa Barbara, CA: ABC-CLIO, 2010); Wall (see note 7).
34 Holt, Smirnova, and Chua (see note 6); Larry Ponemon, "Calculating the Cost of a Data Breach in 2018, the Age of AI and the IoT," *Security Intelligence*, July 11, 2018. https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/; Symantec, "Internet Security Threat Report, 23" (Symantec Security Center, 2018). https://www.symantec.com/security-center/threat-report.
35 Holt, Smirnova, and Chua (see note 6); Rutger E. Leukfeldt, Edward R. Kleemans, and Wouter P. Stol, "Origin, Growth and Criminal Capabilities of Cybercriminal Networks: An International Empirical Analysis," *Crime, Law and Social Change* 67, no. 1 (2017): 39–53.
36 Thomas J. Holt and Max Kilger, "Know Your Enemy: The Social Dynamics of Hacking," *The Honeynet Project* (2012): 1–17.
37 Gabriella Coleman,*Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous* (London, England: Verso Books, 2014).
38 Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," *Networks and netwars: The future of terror, crime, and militancy* 239, (2001): 288; Max Kilger, "Social Dynamics and the Future of Technology-Driven Crime: Social dynamics and implications." (IGI Global, 2011), 205–27; Woo, Kim, and Dominick (see note 4).
39 Ibid.
40 Ibid.
41 Ibid.; Holt, Freilich, and Chermak (see note 23).
42 Holt, Freilich, and Chermak (see note 23).
43 Dorothy E. Denning, "Cyber Conflict as an Emergent Social Phenomenon," in Corporate hacking and technology-driven crime: Social dynamics and implications (IGI Global, 2011) 170–86; Woo, Kim, and Dominick (see note 4).
44 Jason Andress and Steve Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners* (Waltham, MA: Elsevier, 2014); Denning (see note 44).
45 Sean Michael Kerner, "Ddos Attacks: Growing, but How Much," *eSecurity Planet*, April 26, 2013, http://www.esecurityplanet.com/network-security/ddos-attacks-growing-but-how-much.html.
46 Denning (see note 44); Kilger (see note 39).
47 Coleman (see note 38); Parmy Olson, *We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency* (New York: Back Bay Books, 2012).
48 Holt (see note 3); Jordan and Taylor (see note 4).
49 Denning (see note 44); Holt, Smirnova, and Chua (see note 6).
50 Olson (see note 48).
51 Freilich, Chermak, Belli, Gruenewald, and Parkin (see note 5).
52 Andress and Winterfeld (see note 45); Holt (see note 3).
53 Chermak and Gruenewald (see note 26); Freilich, Chermak, Belli, Gruenewald, and Parkin (see note 5).
54 Olson (see note 48).

55 Coleman (see note 38); Denning (see note 44).
56 Holt, Freilich, and Chermak (see note 23); Jordan and Taylor (see note 4); Woo, Kim, and Dominick (see note 4).
57 Chermak and Gruenewald (see note 26).
58 Denning (see note 44); Holt, Smirnova, and Chua (see note 6); Kilger (see note 39).
59 Freilich, Chermak, Belli, Gruenewald, and Parkin (see note 5).
60 Ibid.
61 Ponemon (see note 35); Symantec (see note 35).
62 Department of Homeland Security, *Assessment: Leftwing Extremists Likely to Increase Use of Cyberattacks Over the Coming Decade* (Washington, DC); Holt (see note 3).
63 Kilger (see note 39).
64 Holt, Smirnova, and Chua (see note 6); Ponemon (see note 35).
65 Waqas Amir, "Anonymous Hacks National Agriculture Library Domain for OpMonsanto," *HackRead*, November 8, 2015. https://www.hackread.com/opmonsanto-anonymous-hacks-national-agriculture-library/.
66 Nathan Eagle and Anita Hofschneider, "Cyberattack Hits TMT and State Government Websites," *Honolulu Civil Beat*, April 26, 2015, https://www.civilbeat.org/2015/04/hackers-given-credit-for-shutting-tmt-hawaii-state-websites-down/.
67 Ibid.
68 Denning (see note 39); Foltz, "Cyberterrorism, Computer Crime, and Reality," 154–66; Holt (see note 3); Holt, Freilich, and Chermak (see note 23); Weimann (see note 3).
69 Department of Homeland Security (see note 63); Holt (see note 3).
70 Juliet Eilperin, "As Eco-Terrorism Wanes, Governments Still Target Activist Groups seen as a Threat," *The Washington Post*, March 10, 2012.
71 For an exception, see Department of Homeland Security (see note 63).
72 Brenner (see note 34); Holt and Bossler (see note 7).
73 Coleman (see note 38).
74 Chermak and Gruenewald (see note 26).
75 Foltz (see note 69); Holt (see note 3).
76 Holt and Kilger (see note 37).
77 Holt, Freilich, and Chermak (see note 23); Woo, Kim, and Dominick (see note 4).
78 Jordan and Taylor (see note 4); Kevin F. Steinmetz,*Hacked: A Radical Approach to Hacker Culture and Crime* (New York, NY: New York University Press, 2016).
79 Yar (see note 10).
80 Andress and Winterfeld (see note 45); Holt and Kilger (see note 37); Thomas Rid, *Cyber War Will Not Take Place* (Oxford, UK: Oxford University Press, 2013).
81 Erika Harrell, *Victims of Identity Theft, 2014* (Washington DC: U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Statistics, 2017); Holt and Bossler (see note 7).
82 Department of Homeland Security (see note 63); Holt and Bossler (see note 7).
83 Freilich, Chermak, Belli, Gruenewald, and Parkin (see note 5).
84 Holt and Bossler (see note 7).
85 Holt (see note 3); Holt and Bolden, "Technological Skills of White Supremacists in an Online Forum: A Qualitative Examination," *Journal of Cyber Criminology* 8, 79–93; Weimann (see note 3).
86 Freilich, Chermak, Belli, Gruenewald, and Parkin (see note 5); LaFree, Dugan, and Miller (see note 8).
87 Holt and Bolden (see note 86).
88 Jordan and Taylor (see note 4).
89 Holt and Bossler (see note 7).